JC19 Rec'd PCT/PTO 07 JUN 2001

FORM PTO-1390 (REV. 10-96)	U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE	ATTORNEY DOCKET NUMBER
	TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371	A-70661/MAK
		U.S. APPLICATION NO. (If known, see 37 C.F.R. 1.5) 09/857725 Not Yet Known

NTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/AU99/01096	8 December 1999	8 December 1998

TITLE OF INVENTION

A CERTIFICATION METHOD

APPLICANT(S) FOR DO/EO/US

TELSTRA R & D MANAGEMENT PTY. LTD.

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a FIRST submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a SECOND or SUBSEQUENT submission of items concerning a filing under 35 U.S.C. 371
3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT Articles 22 and 39(1).
4. ☐ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. ☒ A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. ☐ is transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☒ has been transmitted by the International Bureau. **(see enclosed Form PCT/IB/308)**
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US)
6. ☐ A translation of the International Application into English (35 U.S.C. 371(c)(2)).
7. ☐ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☐ have been transmitted by the International Bureau.
   c. ☒ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☐ have not been made and will not be made.
8. ☐ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. ☐ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
10. ☐ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11. to 16. below concern other document(s) or information included:

11. ☐ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. ☐ A FIRST preliminary amendment.
    ☐ A SECOND or SUBSEQUENT preliminary amendment.
14. ☐ A substitute specification.
15. ☐ A change of power of attorney and/or address letter.
16. ☐ Other items or information.

U.S. APPLICATION NO. (If known, see 37 C.F.R. 1.53)	INTERNATIONAL APPLICATION NO.	ATTORNEY'S DOCKET NUMBER
Not Yet Known 09/857725	PCT/AU99/01096	A-70661/MAK

531 Rec'd PCT/PTO 07 JUN 2001

17. ☒ The following fees are submitted:	CALCULATIONS (PTO USE ONLY)	
Basic National Fee (37 CFR 1.492(a)(1)-(5)):		
Search Report has been prepared by the EPO or JPO $860.00		
International preliminary examination fee paid to USPTO (37 CFR 1.482) $690.00		
No international preliminary examination fee paid to USPTO (37 CFR 1.482) but international search fee paid to USPTO (37 CFR 1.445(a)(2)) $710.00		
Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO $1,000.00		
International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(1)-(4) $100.00		
ENTER APPROPRIATE BASIC FEE AMOUNT =	$ 1,000.00	
Surcharge of $130.00 for furnishing the oath or declaration later than ☐ 20 ☒ 30 months from the earliest claimed priority date (37 CFR 1.492(e)).	$ 130.00	

CLAIMS	NUMBER FILED		NUMBER EXTRA	RATE		
Total Claims	44	-20 =	24	18.00	$ 432.00	
Independent Claims	5	-3 =	2	80.00	$ 160.00	
Multiple dependent claims (if applicable)				270.00	$ -0-	
TOTAL OF ABOVE CALCULATIONS =					$ 1,722.00	
Reduction by 1/2 for filing by small entity, if applicable. Applicant claims small entity status. (See 37 CFR 1.27.) Yes: ☐ No: ✓					$ -0-	
SUBTOTAL =					$ 1,722.00	
Processing fee of $130.00 for furnishing the English translation later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(f)). +					$ -0-	
TOTAL NATIONAL FEE =					$ 1,722.00	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). $40.00 per property +					$ -0-	
TOTAL FEES ENCLOSED =					1,722.00	
					Amount to be: refunded	$
					charged	$

a. ☒ A check in the amount of $1,722.00 to cover the above fees is enclosed.

b. ☐ Please charge my Deposit Account No. 06-1300 (Order No.) in the amount of $ _____ to cover the above fees.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 06-1300 (Order No. A-70661/MAK).

NOTE: ***Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.***

SEND ALL CORRESPONDENCE TO:

Michael A. Kaufman, Esq.
FLEHR HOHBACH TEST,
ALBRITTON & HERBERT LLP
Four Embarcadero Center - Suite 3400
San Francisco, California 94111-4187
Tel.: (415) 781-1989
Fax: (415) 398-3249

Robert B Chickering
SIGNATURE

Robert B. Chickering
NAME

24,286
REGISTRATION NUMBER

09857725
PCT/AU99/01096
Rec'd PCT/PTO 07 JUN 200

A CERTIFICATION METHOD

The present invention relates to a certification method and system. The present invention particularly, but not exclusively, relates to public key cryptography and a process for the issuing of digital certificates to bind a person's identity to a particular public key.

The basis of public key cryptography is the generation of a public and private key pair for use in the encryption and decryption, and signing and verifying, of information transmitted over public access communication lines. Key pairs are mathematically related, but it is not practically feasible to derive a private key from its corresponding public key. A person may openly distribute the public key but the person must keep secret the private key. Anyone wishing to send information to a person encrypts the information using that person's public key. The recipient, being the sole possessor of the corresponding private key, is the only person who can decrypt that information.

For a number of electronic commerce applications, a trusted third party, known as a Certification Authority (CA), is needed to bind a person's identity or information, such as privileges, memberships, account numbers, etc., to their public key. The CA issues a digital certificate, which is essentially a form of electronic identification that binds two or more pieces of information, such as the identity of the person and a particular public key. Throughout the specification a reference to person is intended to include a reference to an organisation or individual.

The process of binding a public key to a person must be secure so that the CA can issue a digital certificate and be accordingly held responsible for it. At present, there is a weakness in certification processes used by CAs. Once the CA receives the public key generated by a person's equipment, together with other data concerning the person, a registrar of the CA contacts the person, or vice versa, to correctly identify them with reference to the person's identifying or personal data that has been provided. This is normally done by having the contacted person repeat to the registrar personal details, such as mothers' maiden names and drivers' licence numbers. This identifying information however is only related to the identifying or personal data submitted by the person and does not relate whatsoever to the public key which is used for all future communications. The public key can therefore become separated from the

person's data held by the CA or substituted and there is currently no method of relating the public key to the person other than by storing it with the person's data. It is desired to overcome this problem or at least provide a useful alternative.

The present invention provides a certification method, including:

receiving a public key of a public/private key pair generated by a system of a person;

processing said public key to generate a communicable code representative of said public key;

identifying said person, said identifying including having said person convey said communicable code; and

generating a digital certificate, said certificate including said public key.

The present invention also provides a certification system, including:

means for receiving a public key of a public/private key pair generated by a system of a person;

means for processing said public key to generate a communicable code representative of said public key; and

means for generating a digital certificate after identifying said person, said identifying including having said person convey said communicable code, and said certificate including said public key.

The present invention also provides a certification program stored on computer readable storage media, including:

code for receiving a public key of a public/private key pair generated by a system of a person;

code for processing said public key to generate a communicable code representative of said public key; and

code for generating a digital certificate after identifying said person, said identifying including having said person convey said communicable code, and said certificate including said public key.

The present invention also provides an identification process, including:

receiving a public key of a public/private key pair and identifying information of a

person;

deriving a communicable code from said public key; and

having said person convey said communicable code.

The present invention also provides an identification process, including:

generating a communicable code from a public key of a public/private key pair; and

binding said public key to identifying information of a person when said person conveys said communicable code.

A preferred embodiment of the present invention is hereinafter described, by way of example only, with reference to the accompanying drawings, in which:

Figure 1 is a block diagram of a preferred embodiment of a certification system; and

Figure 2 is a flowchart of steps executed by the system.

Referring to Figure 1, there is shown a person 20 who can interact with a telephone 42 or the person's computer system 32. The computer system 32 can communicate with a certification computer system 30 of a Certification Authority (CA), or a registrar acting for or on behalf of the CA, via a communications channel 60. A registrar 10 of the CA interacts with the certification system 30 and a telephone 40 to communicate with and confirm the identity of the person 20. The registrar 10 and the person communicate verbally over a communications channel 62 connecting the telephones 40, 42. The computer systems 30, 32 may communicate with each other independently or on instructions from the registrar 10 or person 20, respectively. The communications channels 60, 62 may be constituted by any voice or data transmission media. For example, the communications channel 60 may be a TCP/IP link.

Referring to Figure 2, a person wishing to obtain a certificate from the CA would visit the CA web site 100 using the person's computer system 32. This is the first step in the process of obtaining a certificate and is one way by which the person may perform the second step of filling out the registration form 110 and sending it to the CA over the communications channel 60. The registration form captures personal or identifying information about the person which could be used to confirm the identity of that person over the telephone. Once the person fills out and sends the registration form 110, the person is not aware of the subsequent steps in the process until he or she receives a registration ID, at step 210, in the form of a communicable

code. The intervening parts 120 to 200 of the process are conducted by the computer systems 30, 32 automatically.

The computer system 30 of the CA receives and processes the submitted registration form at step 120 and sends an instruction to generate the public/private key pair 130 to the computer system 32 of the person. The received registration information may be stored in a database at this point or may be stored once the person's public key is received and the corresponding alphanumeric code is generated together with that information. Once the computer system 32 has received the instruction to generate a public/private key pair, it generates, according to algorithms commonly used by browser applications, such as Netscape Navigator or Microsoft Internet Explorer, a public/private key pair at step 140. The private key is kept securely by the person in the memory of the computer system 32 or another data storage medium, while the public key may be used by anyone wishing to send information to the person. The person's computer system 32 sends the public key 150 to the computer system 30 of the CA. Once the computer system 30 receives the public key it generates the communicable code, at step 180. The public key is represented as a value of the Abstract Syntax Notation No. 1 (described in ASN.1 by ITU) data type SubjectPublicKeyInfo (defined in standard X.509 by ITU), encoded according to the distinguished encoding rules (DER by ITU) and passed through a secure one-way hash algorithm such as SHA-1 (defined in the U.S. Government Federal Information Processing Standard (FIPS) 180-1). The output of the hash algorithm is truncated to 40 bits and converted to 8 base-32 characters. The numerals and upper case letters (excluding '0', '1', 'O' and 'I' to avoid confusion) are used as the base-32 character set. For example, the code may be 8JQ3 UEB5. The code is communicable, to the extent that it is sensibly communicable by the person to the registrar on the communications channel 62, which may include a telephone call or facsimile message. The public key is not sensibly communicable on an identification channel 62 as it is a large mathematical quantity typically consisting of hundreds of decimal digits. The information on the person generated and received is then stored in a database, at step 190, by the CA.

The communicable alphanumeric code is sent to the person as a registration ID, at step 200. The person will probably not know that the registration ID is, in fact, derived from the public key generated by the person's computer system 32. At some time after the person receives the registration ID 210, he or she establishes telephone communication with the

registrar of the CA and provides the registrar with relevant person identification information, at step 220. The registrar confirms the relevant information 230 and requests the person to say the registration ID 240. Once the person provides the registration ID 250 to the registrar, the CA has a public key from computer system 30 and a confirmed identity and communicable code from the registrar. The CA compares, at step 260, the code to a value recalculated from the public key using the secure hash algorithm and, if they match, issues a digital certificate that lists the public key and confirmed identity 270. The digital certificate thereby incorporates the public key and the confirmed identity data and is signed by the CAs private key. The certificate may be sent, at step 280, to the person and stored, at step 290, on their hard drive, floppy disk, smart card, etc. and/or the certificate may be published in another system, such as electronic white pages.

As the alphanumeric code used in the identification process is derived directly from the public key, the CA can ensure the identification information confirmed by the registrar and the public key are bound as a pair, which ensures the digital certificate contains the correct information.

The steps of the certification process described above which are executed on the computer systems 30 and 32 are preferably executed by, or under the control of, computer programs resident on the respective systems 30 and 32. The steps may also be wholly or partly executed by dedicated hardware included in the systems, such as application specific integrated circuits (ASICs). The systems 30 and 32 may comprise single systems in one location or may comprise distributed systems with their software and hardware components in different locations.

Many modifications will be apparent to those skilled in the art without departing from the scope of the present invention as herein described. For example, the person 20 being identified may be aware that the registration ID is a summary of the public key. Their system 32 could be used to generate the alphanumeric code, which acts as a key summary, and the person can then convey the code with the identifying information which is to be bound to the public key. Also when the registrar identifies the person and has the person convey the communicable code, a number of techniques could be employed to initiate or achieve this. For example, the registrar may phone the person, the person may phone the registrar, as discussed

above, or the person can physically visit, fax or send mail to the registrar, and/or vice versa.

5

CLAIMS:

1. A certification method, including:

receiving a public key of a public/private key pair generated by a system of a person;

processing said public key to generate a communicable code representative of said public key;

identifying said person, said identifying including having said person convey said communicable code; and

generating a digital certificate, said certificate including said public key.

2. A certification method as claimed in claim 1, wherein said identifying includes verifying identification information of said person, and said certificate binds said identifying information and said public key.

3. A certification method as claimed in claim 2, wherein said communicable code is a limited character string.

4. A certification method as claimed in claim 3, wherein said communicable code is generated using a secure one-way hash function.

5. A certification method as claimed in claim 1, including requesting generation of the public/private key pair by the system of the person, in response to receiving a registration request from the person.

6. A certification method as claimed in claim 5, wherein said registration request includes said identifying information for said person.

7. A certification method as claimed in claim 1, wherein said identifying includes matching a communicable code generated from said public key with the communicable code conveyed by said person.

8. A certification method as claimed in claim 1, including sending said digital certificate to said system of said person.

9. A certification method as claimed in claim 1, including sending said code to said system for said person.

10. A certification method as claimed in claim 9, wherein said sending includes transmitting display data to said system for display of said communicable code by said system.

11. A certification method as claimed in claim 1, wherein said processing of said public key is executed by said system of said person.

12. A certification method as claimed in claim 1, wherein said conveying involves oral communication of said communicable code.

13. A certification method as claimed in claim 12, wherein the oral communication occurs during a telecommunications call.

14. A certification system, including:

means for receiving a public key of a public/private key pair generated by a system of a person;

means for processing said public key to generate a communicable code representative of said public key; and

means for generating a digital certificate after identifying said person, said identifying including having said person convey said communicable code, and said certificate including said public key.

15. A certification system as claimed in claim 14, wherein said identifying includes verifying identification information of said person, and said certificate binds said identifying information and said public key.

16. A certification system as claimed in claim 15, wherein said communicable code is a limited character string.

17. A certification system as claimed in claim 16, wherein said communicable code is generated using a secure one-way hash function.

18. A certification system as claimed in claim 14, including means for sending said code to said system for said person.

19. A certification system as claimed in claim 14, including means for requesting generation of the public/private key pair by the system of the person, in response to receiving a registration request from the person.

20. A certification system as claimed in claim 19, wherein said registration request includes said identifying information for said person.

21. A certification system as claimed in claim 14, wherein said identifying includes matching a communicable code generated from said public key with the communicable code conveyed by said person.

22. A certification system as claimed in claim 14, including means for sending said digital certificate to said system of said person.

23. A certification system as claimed in claim 18, wherein said means for sending transmits display data to said system for display of said communicable code by said system.

24. A certification system as claimed in claim 14, wherein said conveying involves oral communication of said communicable code.

25. A certification system as claimed in claim 24, wherein the oral communication occurs during a telecommunications call.

26. A certification system as claimed in claim 14, including means for executing said identifying.

27. A certification program stored on computer readable storage media, including:

code for receiving a public key of a public/private key pair generated by a system of a person;

code for processing said public key to generate a communicable code representative of

said public key; and

code for generating a digital certificate after identifying said person, said identifying including having said person convey said communicable code, and said certificate including said public key.

28. A certification program as claimed in claim 27, wherein said identifying includes verifying identification information of said person, and said certificate binds said identifying information and said public key.

29. A certification program as claimed in claim 28, wherein said communicable code is a limited character string.

30. A certification program as claimed in claim 29, wherein said communicable code is generated using a secure one-way hash function.

31. A certification program as claimed in claim 27, including code for sending said code to said system for said person.

32. A certification program as claimed in claim 27, including code for requesting generation of the public/private key pair by the system of the person, in response to receiving a registration request from the person.

33. A certification program as claimed in claim 32, wherein said registration request includes said identifying information for said person.

34. A certification program as claimed in claim 27, wherein said identifying includes matching a communicable code generated from said public key with the communicable code conveyed by said person.

35. A certification program as claimed in claim 27, including code for sending said digital certificate to said system of said person.

36. A certification program as claimed in claim 31, wherein said code for sending transmits

display data to said system for display of said communicable code by said system.

37. A certification program as claimed in claim 27, wherein said conveying involves oral communication of said communicable code.

38. A certification program as claimed in claim 37, wherein the oral communication occurs during a telecommunications call.

39. A certification program as claimed in claim 27, including code for executing said identifying.

40. An identification process, including:

receiving a public key of a public/private key pair and identifying information of a person;

deriving a communicable code from said public key; and

having said person convey said communicable code.

41. An identification process as claimed in claim 40, including comparing a communicable code derived from the public key with the conveyed communicable code, and issuing a digital certificate binding the public key and identifying information when the codes match.

42. An identification process as claimed in claim 41, wherein said communicable code is a limited character string.

43. An identification process as claimed in claim 42, wherein said communicable code is generated using a secure one-way hash function.

44. An identification process, including:

generating a communicable code from a public key of a public/private key pair; and

binding said public key to identifying information of a person when said person conveys said communicable code.

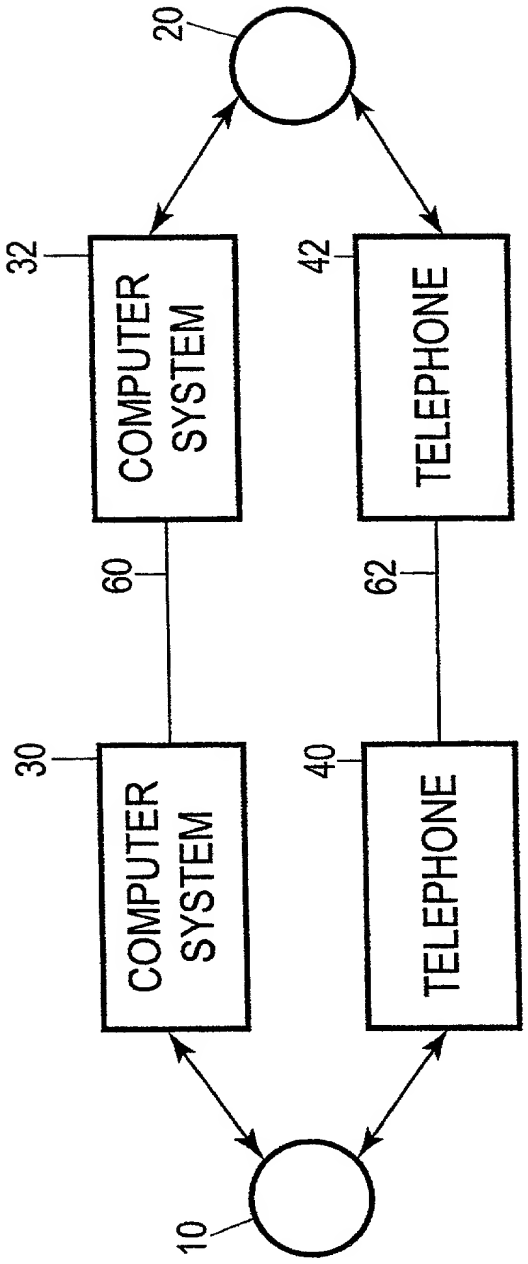
20
32
COMPUTER SYSTEM
42
TELEPHONE
60
62
30
COMPUTER SYSTEM
40
TELEPHONE
10

FIG 1

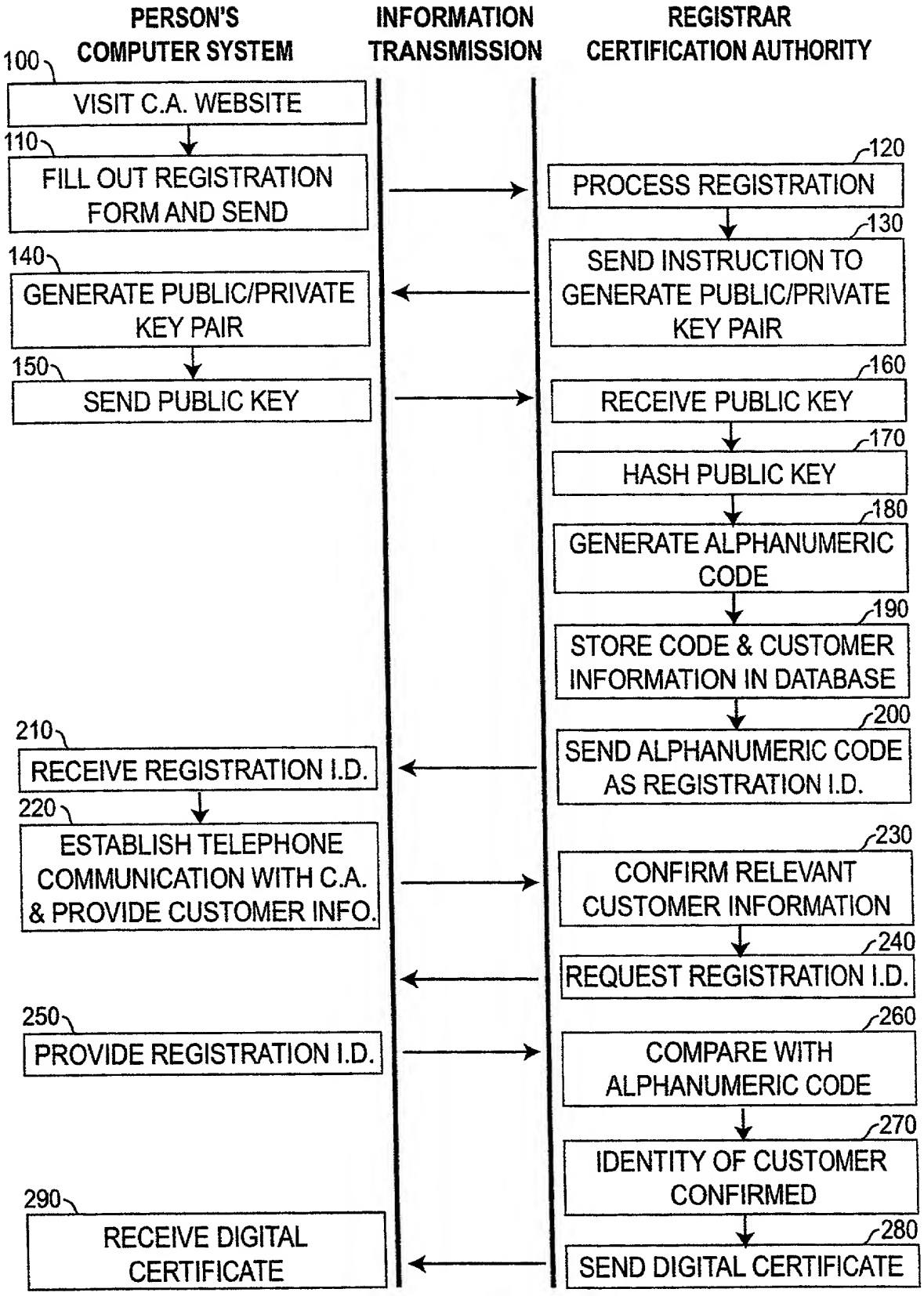
PERSON'S COMPUTER SYSTEM
INFORMATION TRANSMISSION
REGISTRAR CERTIFICATION AUTHORITY
100
VISIT C.A. WEBSITE
110
FILL OUT REGISTRATION FORM AND SEND
120
PROCESS REGISTRATION
130
SEND INSTRUCTION TO GENERATE PUBLIC/PRIVATE KEY PAIR
140
GENERATE PUBLIC/PRIVATE KEY PAIR
150
SEND PUBLIC KEY
160
RECEIVE PUBLIC KEY
170
HASH PUBLIC KEY
180
GENERATE ALPHANUMERIC CODE
190
STORE CODE & CUSTOMER INFORMATION IN DATABASE
200
SEND ALPHANUMERIC CODE AS REGISTRATION I.D.
210
RECEIVE REGISTRATION I.D.
220
ESTABLISH TELEPHONE COMMUNICATION WITH C.A. & PROVIDE CUSTOMER INFO.
230
CONFIRM RELEVANT CUSTOMER INFORMATION
240
REQUEST REGISTRATION I.D.
250
PROVIDE REGISTRATION I.D.
260
COMPARE WITH ALPHANUMERIC CODE
270
IDENTITY OF CUSTOMER CONFIRMED
280
SEND DIGITAL CERTIFICATE
290
RECEIVE DIGITAL CERTIFICATE

FIG 2

DECLARATION AND POWER OF ATTORNEY
FOR PATENT APPLICATION

As a below-named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled A CERTIFICATION METHOD

the specification of which

(check one) ☐ is attached hereto.

☒ was filed on 7 June, 2001 as Application Serial No. 09/857,725 and was amended on _____ (if applicable).

[X] International Patent Application No PCT/AU99/01096 filed 8 Dec. 1999

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, §1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)			Priority Claimed	
PP7570/98	Australia	8 December 1998	☒	☐
(Number)	(Country)	(Day/Month/Year Filed)	Yes	No
PCT/AU99/01096	PCT	8 December 1999	☒	☐
(Number)	(Country)	(Day/Month/Year Filed)	Yes	No
_____	_____	_____	☐	☐
(Number)	(Country)	(Day/Month/Year Filed)	Yes	No

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulation, §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

(Application Serial No.)	(Filing Date)	(Status) (patented, pending, abandoned)
(Application Serial No.)	(Filing Date)	(Status) (patented, pending, abandoned)

16

I hereby appoint the following attorneys to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith: Harold C. Hohbach, Reg. No. 17,757; Aldo J. Test, Reg. No. 18,048; Thomas O. Herbert, Reg. No. 18,612; Donald N. MacIntosh, Reg. No. 20,316; Jerry G. Wright, Reg. No. 20,165; Edward S. Wright, Reg. No. 24,903; David J. Brezner, Reg. No. 24,774; Richard E. Backus, Reg. No. 22,701; James A. Sheridan, Reg. No. 25,435; Robert B. Chickering, Reg. No. 24,286; Willis E. Higgins, Reg. No. 23,025; Gary S. Williams, Reg. No. 31,066; Richard F. Trecartin, Reg. No. 31,801; Stephen C. Durant, Reg. No. 31,506; C. Michael Zimmerman, Reg. No. 20,451; Walter H. Dreger, Reg. No. 24,190; _____;

provided that if any one of said attorneys ceases being affiliated with the law firm of Flehr, Hohbach, Test, Albritton & Herbert as partner, employee or of counsel, such attorney's appointment as attorney and all powers derived therefrom shall terminate on the date such attorney ceases being so affiliated.

Direct all telephone calls to Michael A. Kaufman at (415) 781-1989.

Address all correspondence to:

FLEHR, HOHBACH, TEST,
ALBRITTON & HERBERT
Suite 3400, Four Embarcadero Center
San Francisco, California 94111

File No. A-70661/MAK

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Title 18, United States Code, §1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

1-00

Full name of sole or first inventor: James Howard MANGER

Inventor's signature: × James Manger

Date: × 11 July 2001

Residence: Carlton North, Victoria, Australia

Citizenship: Australian

Post Office Address: Flat 6, 623 Drummond Street, Carlton North, Victoria 3054, Australia

2-00

Full name of second joint inventor, if any: Edward Andrew ZUK

Inventor's signature: × Edward Zuk

Date: × 27 July 2001

Residence: Elwood, Victoria, Australia

Citizenship: Australian

Post Office Address: 1 Heaton Avenue, Elwood, Victoria 3184, Australia